

REMARKS

Applicant requests favorable reconsideration and allowance of this application in view of the foregoing amendments and the following remarks.

Claims 1-3, 5-14, 17 and 18 are pending in this application, with Claims 1, 5, 9, 11, 13, 17, and 18 being independent. Claims 4, 15, and 16 have been cancelled herein without prejudice.

Claims 1, 9, 11 and 17 have been amended. Applicant submits that support for the amendments can be found in the original disclosure at least, for example, at page 21, lines 12-22 of the specification. Therefore, Applicant submits that no new matter has been added.

The Drawings were objected to as allegedly failing to comply with 37 C.F.R. §1.84(p)(5) for failing to include the reference sign "patent document 1" mentioned at page 4 of the specification. Applicant respectfully submits that "patent document 1" is not a reference character referring to a part of the disclosed invention. Instead, "patent document 1" is a name used to refer a document discussed in the specification. Specifically, at page 4, lines 4-5, the specification says, "Japanese Patent Application Laid-Open No. 2001-105690 (hereinafter called a patent document 1)." Accordingly, Applicant submits that it is neither required nor appropriate for the drawings to include "patent document 1," and withdrawal of the objection to the drawings is requested.

Claims 1-18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,378,070 (Chan) in view of U.S. Patent No. 6,360,320 (Ishiguro). Applicant respectfully traverses this rejection for the reasons discussed below.

As recited in independent Claim 1, the present invention includes, *inter alia*, the features of a random number generation unit adapted to generate a random number and a print data encryption unit adapted to encrypt print data using the random number as an encryption key. The invention of Claim 1 also includes the features of a code reception unit adapted to receive a personal identification code input by a user, a code conversion unit adapted to convert the received personal identification code by using a predetermined function, and a random number encryption unit adapted to encrypt the generated random number by using the personal identification code or the converted personal identification code. Claim 1 further recites the feature of a transmission unit adapted to transmit the encrypted random number, the converted personal identification code, and the encrypted print data to a print control apparatus.

Due to the above-mentioned features of Claim 1, since it is the personal identification code converted by the code conversion unit that is transmitted to the print control apparatus, the personal identification code itself is never transmitted on a network in plain text. Consequently, it is possible to prevent the personal identification code from becoming known by a third party, and therefore it is possible to significantly upgrade security for the random number encrypted based on the personal identification code. Furthermore, it is possible to significantly upgrade security for the print data encrypted based on the random number.

Applicants submit that the cited art fails to disclose or suggest the above-mentioned features of Claim 1. Chan discloses a technique of upgrading security in a case where a document created by a host PC is printed by a printer. More specifically, in Chan, a directory server 120, which manages a public key in correspondence with identification information of a user, is provided on a network. A host PC 100 encrypts PDL data (page description language

data) being sent as print data by using a random number as a key, transmits the identification information of the user who receives the document to the directory server 120, obtains from the directory server 120 the public key of the user who receives the document, and then encrypts the random number by using the obtained public key as the encryption key. Further, the host PC 100 transmits the PDL data encrypted by using the random number as the encryption key, the random number encrypted by using the public key, and the identification information of the user who receives the document to a storage 130.

Applicant submits, however, that Chan fails to disclose or suggest at least the features of converting a received personal identification code by using a predetermined function, and transmitting the converted personal identification code together with the encrypted random number and the encrypted print data. Instead, the public key used in Chan to encrypt the random number is merely obtained from the directory server 120, but it is not converted by using a predetermined function, as recited in Claim 1. Further, the public key used in Chan to encrypt the random number is not transmitted together with the encrypted random number, but instead Chan merely transmits information identifying the user who receives the document.

Applicant submits that these differences between Chan and the invention of Claim 1 are not merely trivial differences but instead provide a real advantage. Since Chan protects the random number used to encrypt the PDL data by encrypting the random number using the public key of the user who receives the document, it is necessary to provide a directory server for managing the public keys, from which the public key of the user who receives the document can be obtained. On the other hand, in the present invention recited in Claim 1, since the random number used to encrypt the print data is protected by encrypting the random number based on a

personal identification code input by the user (either by using the personal identification code or a converted personal identification code), and the converted personal identification code is transmitted along with the encrypted random number, it is possible to easily/simply achieve the mechanism for protecting the random number (and consequently protecting the encrypted print data) without providing a directory server or the like for managing public keys.

Applicant submits that Ishiguro likewise fails to disclose or suggest at least the above-mentioned features and fails to remedy the above-noted deficiencies of Chan. Ishiguro discloses a technique of converting data according to a hash function. In the system of Chan, there is no conversion of either the public key used to encrypt the PDL data or the identification information indicating the user to whom the document is transmitted (and with whom the public key is associated). Moreover, in the system of Chan, since the random number is encrypted by using a public key, there is no need to convert either the public key or the identification information of the user. A public key is not secret, and there is no indication that the identity of the user to whom the document is transmitted is intended to be kept secret, so there is no reason to perform any conversion and the information can be transmitted in plain text.

For the foregoing reasons, Applicant submits that the present invention recited in independent Claim 1 is patentable over the art of record, whether that art is taken individually or considered in combination.

Independent Claims 9, 11, and 17 recite features similar to some of the above-discussed features of Claim 1, and those claims are believed patentable for reasons similar to Claim 1.

The present invention as recited in independent Claims 5, 13 and 18 also recites a feature relating to converting a personal identification code by using a predetermined function. As

discussed above with respect to Claims 1, 9, 11, and 17, the system of Chan does not perform any conversion, and it also does not include any data where conversion using a hash function, as disclosed in Ishiguro, would be necessary or appropriate. Accordingly, the invention of Claims 5, 13, and 18 is believed patentable for reasons similar to Claims 1, 9, 11, and 17.

The dependent claims are patentable for at least the same reasons as the independent claims, as well as for the additional features they recite.

In view of the foregoing, Applicant submits that this application is in condition for allowance. Favorable reconsideration and an early Notice of Allowance are requested.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicant
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK/lcw

FCHS_WS 2642976_1